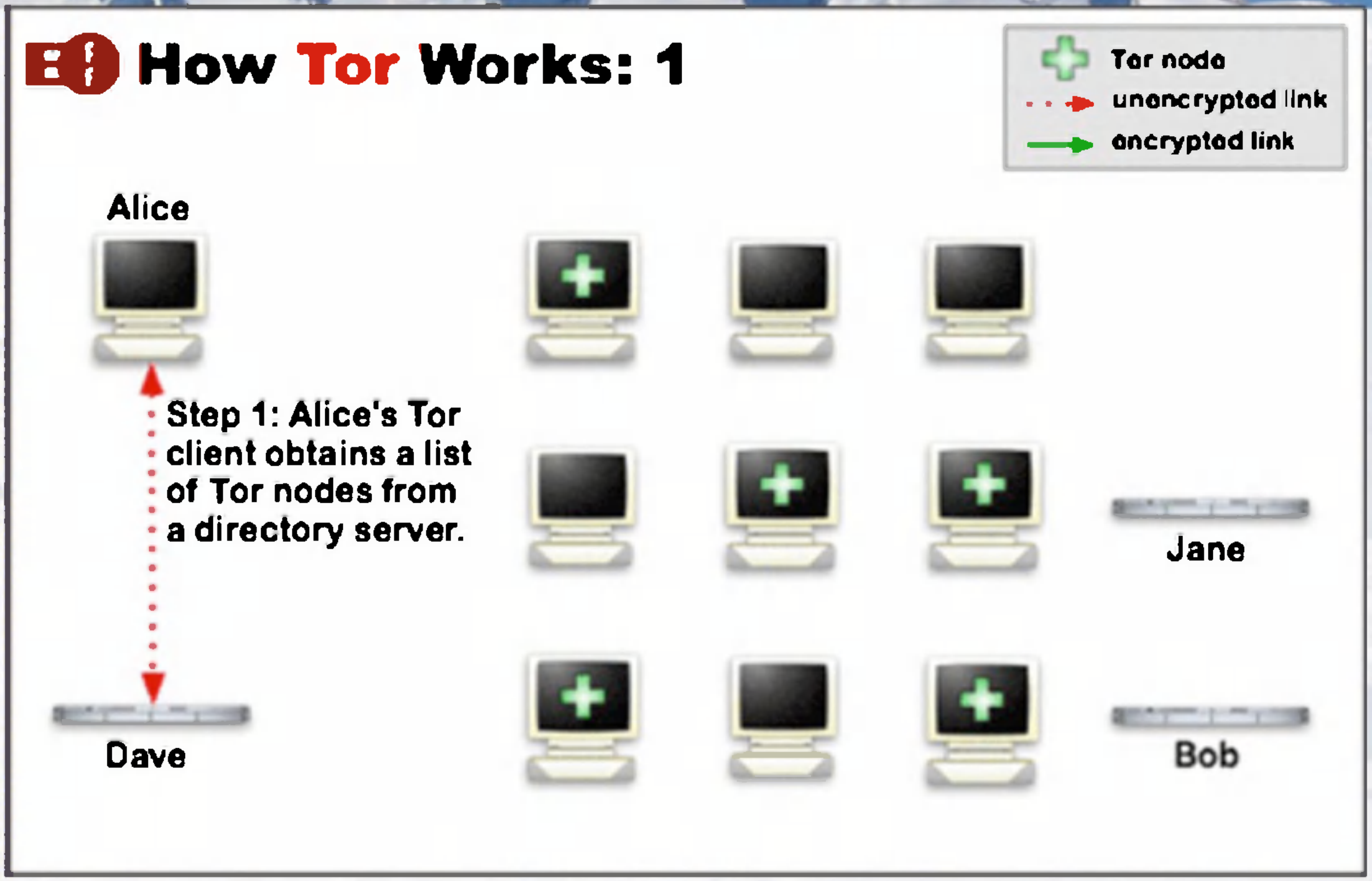
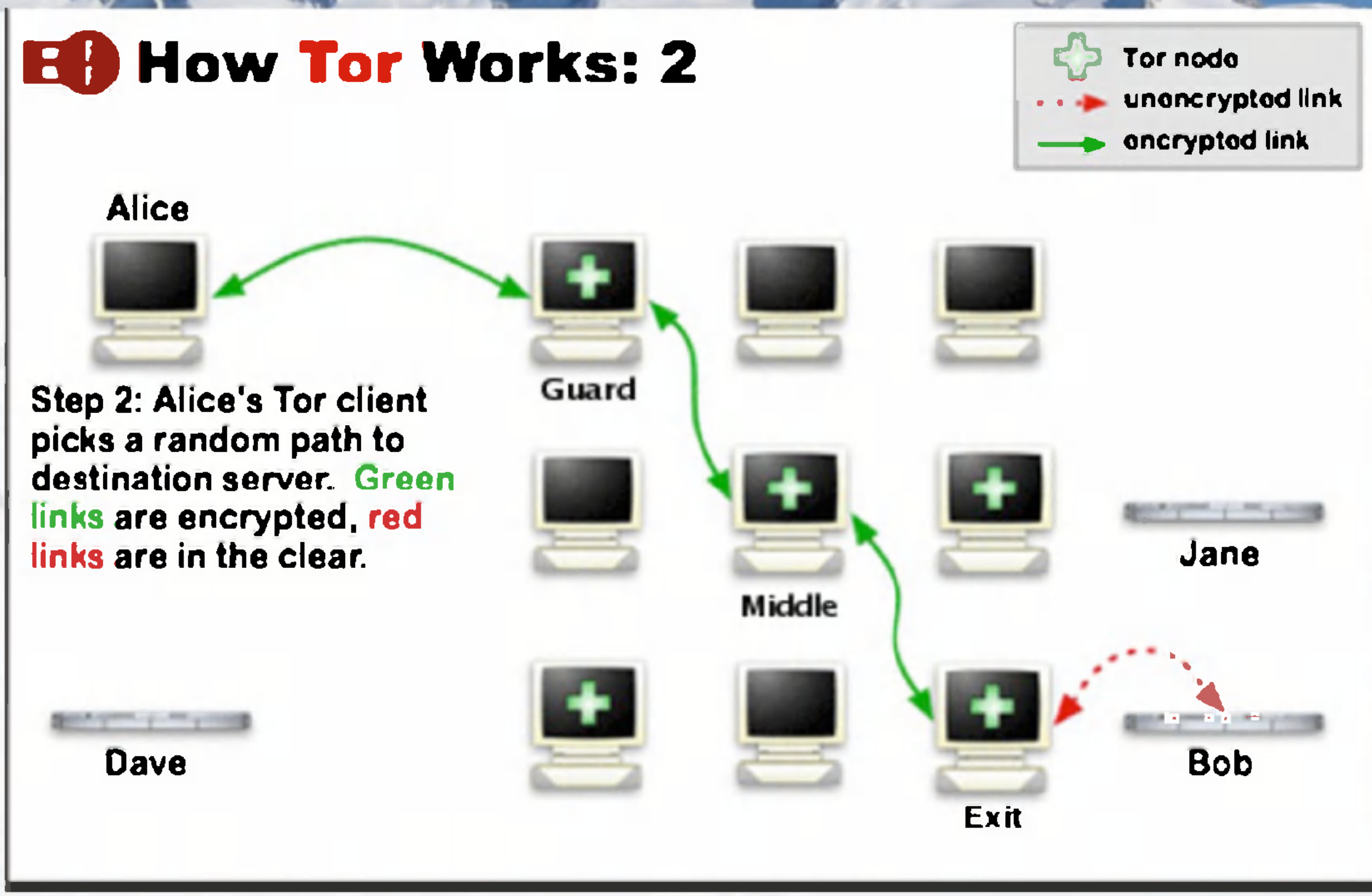
(C//REL) Types of IAT – Advanced Open Source Multi-Hop

- (S//REL) Open Source Multi-Hop Networks
  - (S//REL) *Tor*
  - (S//REL) Very widely used worldwide
  - (S//REL) Open Source
    - (S//REL) Active Development
    - (S//REL) Mitigates Threats
  - (S//REL) Very Secure
  - (S//REL) Low enough latency for most *TCP* uses
  - (S//REL) Still the King of high secure, low latency Internet Anonymity
    - (S//REL) There are no contenders for the throne in waiting

(S//REL) *Tor* Operation (1)



(S//REL) *Tor* Operation (2)



(S//SI//REL) Passive *Tor* Traffic Analysis

- (S//SI//REL) For Normal SIGINT flow, need to identify *Tor* traffic!
  - (S//SI//REL) Only outer *TLS* layer visible → How to Distinguish?
  - (S//SI//REL) *Tor* developers attempt to remain anonymous by blending in with myriad other *TLS* traffic
  - (S//SI//REL) *Tor TLS* has changed over the years
  - (S//SI//REL) There ARE some server → client features which are recognizable
    - (S//SI//REL) Certificate: Specific *Diffie-Hellman* (*DH*) Modulus – byte search
    - (S//SI//REL) Certificate: Issuer and Subject random names of same form – ex: *CN=www.ofzfkdjxvrss.net* – regex match
    - (S//SI//REL) Certificate: always 2 hour lifetime – *ASN.1* parsing, more computation
    - (S//SI) Multiple XKS fingerprints from multiple parties deployed

(S//REL) *Tor* Project Censorship Driven Activity

- (S//REL) Driven by Censorship Circumvention, Hide Signature
  - (S//REL) China and Iran still main adversaries
  - (S//REL) Researching better bridge distribution strategies
    - (S//REL) Claim by *Tor Project* is 8000 requests/day for <1000 total
  - (S//REL) Around Feb 2011, changed the *TLS* handshake
    - (S//REL) Signature more like *Apache* web-server
      - (S//REL) Different *DH* Modulus
      - (S//SI//REL) New XKS Signatures address this
  - (TS//SI//REL) Proposed eventual change will kill identification!
    - (S//REL) Each *Tor* node will generate random-ish signatures in a volatile way specifically designed to look like normal website *TLS* traffic!

(S//REL) Censorship Driven Protocol Obfuscation – *Psiphon 3 / Tor*

(S//REL) Extreme Censorship blocking: Common encrypted protocols

- (S//REL) In the case of *Psiphon 3*: *SSH*
- (S//REL) In the case of *Tor*: *TLS*
- (S//REL) Make deep packet inspection (*XKS* :-)) work harder
- (S//REL) Both use work of a open source project (brl/obfuscated-openssh)

(S//REL) Idea is both sides transmit random seed and verifier information

- (S//REL) Verifier is hash of seed and other data
- (S//REL) If verifier passes data used from both side seeds to generate key
- (S//REL) Key used in symmetric cipher to encrypt native *SSH* or *SSL* protocol
- (S//REL) So for random stream, need to de-obfuscate and test for *SSH / SSL*

(S//REL) Details for *Psiphon 3*

- (S//REL) Hash used for verifier, key generation: 6000 iterations *SHA-1*
- (S//REL) Symmetric cipher is *RC-4*

(S//REL) Details for *Tor Obsfproxy*

- (S//REL) Hash used for verifier, key generation: 100K iterations *SHA-256*
- (S//REL) Symmetric cipher is *AES-CTR-128*
- *(S//REL)* Key uses seed from both sides!

(S//REL) *Tor* Project and friends Recent Activity

- (S//REL) *Tor* on non-traditional platforms
  - (S//REL) *ORBOT*, *Tor* for *Android* smartphones – Associated browser, easy to use!
  - (S//REL) *Tor* Router Project – Modified *Linksys* Router (everything over *Tor*)
  - (S//REL) *Hide-My-IP-Address*
    - (S//REL) Proprietary replacement for *Tor Browser Bundle*
    - (S//REL) From "*WCCL Network*" not part of *Tor* Project
    - (S//SI//REL) Looked at based on reference by CT target
  - (S//REL) *Tor* Project working on improving support for circumvention
    - » (S//REL) Handshake obfuscation (discussed)
    - » (S//REL) Better bridge proliferation / distribution
  - (S//REL) *Tails*: Complete Bootable OS on CD for anonymity – includes *Tor*
    - (S//REL) Adds Severe CNE misery to equation
    - (S//SI//REL) Has been discussed by CT targets

(S//REL) *Tor* Project and friends Recent Activity

- (S//REL) Advanced *Tor* "Obfuscation" Project: *SkypeMorph*
  - (S//REL) Another option for pluggable transport
  - (S//REL) More sophisticated concept than *Obfsproxy*
  - (S//REL) Open connection to Skype server with "bridge *Skype* ID"
  - (S//REL) Encapsulate *Tor* in encrypted data mimicking *Skype* Video Traffic
  - (S//REL) Sort of traffic flow steganography vice content steganography
  - (S//REL) True Public Key cryptography vice obfuscation with known key
  - (S//REL) Product of University research – Non-trivial to deploy
- (TS//SI//REL) Most Recent SIGINT Work on Exploiting *Tor*
  - (TS//SI//REL) REMATION II Workshop (US/UK) at MHS spring 2012
  - (S//SI//REL) Unleashed Networking/CNE legions...
  - (S//REL) See later talk by [redacted] for the scoop

(S//REL) *Tor* Project and friends Recent Activity

- (S//REL) Online Feud between 2 IAT Products: *Ultrasurf* and *Tor*
  - (S//REL) " Technical Analysis of the *Ultrasurf* proxying software" (Applebaum)
    - (S//REL) Analysis (including some SRE) – highly critical
    - (S//REL) Single hop, controlled by one authority
    - (S//REL) Security by obscurity
    - (S//REL) No perfect forward secrecy (forensic traces exploitable)
    - (S//REL) Responsible Disclosure: *Ultrasurf* notified 12/2011, published 04/2012
  - (S//REL) "*Tor*'s critique of *Ultrasurf*: A reply from the *Ultrasurf* developers"
    - » (S//REL) Posted on *Ultrasurf* site days after *Tor* published critique
    - » (S//REL) All talk and no show
    - » (S//REL) Not fully analyzed
    - » (S//REL) One Approach to IAT: *Tor* – higher anonymity, smaller scale
    - » (S//REL) One Approach to IAT: *Ultrasurf* – focus on circumvention, massive scale